Cybersecurity Plan Guidance

Section 40126 of the Infrastructure Investment and Jobs Act (IIJA), also known as the Bipartisan Infrastructure Law (BIL), authorizes the Secretary of Energy to require that certain projects funded under the law include a cybersecurity plan. This guidance document provides information about the cybersecurity plan that selectees may have to submit to the Office of Clean Energy Demonstrations (OCED) prior to receiving funding.

What is a Cybersecurity Plan?

A cybersecurity plan specifies the policies, processes, and controls required to protect an organization against cyber threats and risk. The Department of Energy (DOE) has created three templates to assist you in drafting your plan: one for high risk projects, one for medium risk projects, and one for low risk projects. The templates provide guidance on how to structure a comprehensive plan that meets a project's risk profile. DOE uses cybersecurity plans to promote effective integration and coordination across its research, development, and demonstration programs.

When is a Cybersecurity Plan required?

The Grants and Agreements Officer assigned to your project will send you a letter with a due date and instructions on submitting your cybersecurity plan to OCED's Secure Portal for Cybersecurity Plan Submission. OCED's Independent Data, Engineering, and Analysis Division will work with DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), which is the designated office responsible for reviewing cybersecurity project plans for IIJA-funded projects. CESER coordinates with DOE National Laboratories Subject Matter Experts (SMEs) to provide support activities that maintain or improve the project's cybersecurity over its lifecycle. OCED and CESER will review your plan to ensure program-wide security requirements are met.

The letter will provide a cybersecurity plan template based on the project's risk level. For additional information on the BIL cybersecurity requirements and the cybersecurity plan templates visit Bipartisan Infrastructure Law Implementation page on the CESER website.

Where do I submit the Cybersecurity Plan?

The cybersecurity plan and all related deliverables must be securely transmitted to OCED's Secure Portal for Cybersecurity Plan Submission. Documents uploaded through this page are automatically stored in a secure DOE-managed space that may only be accessed by DOE personnel who are approved to review cybersecurity documentation.

How to create a Cybersecurity Plan?

DOE recommends using the open guidance and standards in the cybersecurity plan templates provided by CESER. Your cybersecurity plan should document any deviation from referenced cybersecurity standards, as well as the utilization of proprietary standards where you deem it necessary.

This guidance document does not supersede Federal laws and regulations. This OCED guidance document is for informational purposes only and is not a requirements document. If there are inconsistencies between this OCED guidance document and any specific program or project document, the specific OCED program or project document should be relied upon as it is the controlling document.

According to Section 40126(b) of the BIL,[1] a cybersecurity plan should describe how the selectee:

- Plans to maintain cybersecurity between networks, systems, devices, applications, or components –
  - within the proposed solution of the project; and
  - at the necessary external interfaces at the proposed solution boundaries;
- Will perform ongoing evaluation of cybersecurity risks to address issues as the issues arise throughout the life of the proposed solution;
- Will report known or suspected network or system compromises of the project to the Secretary; and
- Will leverage applicable cybersecurity programs of the Department, including cyber vulnerability testing and security engineering evaluations.

In general, a cybersecurity plan should be commensurate to the threats and vulnerabilities associated with the proposed efforts and demonstrate the cybersecurity maturity of the project. It may cover a range of topics relevant to the proposed project(e.g., software development lifecycle, third-party risks, and incident reporting). Lastly, a cybersecurity plan should build off an organization's existing cybersecurity program but must also align with project requirements.

During negotiations, selectees are encouraged to attend training with CESER on how to complete their cybersecurity plan. OCED will coordinate training as applicable. During the project's lifecycle, technical assistance will be available for medium and high-risk projects. The project team is responsible for developing, maintaining, and refining the cybersecurity plan and ensuring it is consistent with your organization's evolving cybersecurity program. The plan should include regular reviews and audits to confirm it is up to date with current risks and possible mitigations.

What are the priorities for a Cybersecurity Program?

The selectee's project level cybersecurity plan is derived from and informed by their organization's cybersecurity program. A cybersecurity program is a structured approach to planning, developing, and maintaining levels of information security and risk appropriate to an organization's mission and phase. A selectee should keep in mind their organization's mission, goals, and cybersecurity program when developing their cybersecurity plan. Other considerations are the project's size, complexity, budget, and data management plan, as well as geographic and institutional distribution.

The confidentiality, availability, and integrity of information and information systems has raised the importance of cybersecurity considerations. Cybersecurity protects the availability of instruments and systems; promotes trust in, and availability of, data; and provides confidence in the integrity of the resulting work. At the same time, inappropriate, inefficient, and ineffective cybersecurity compliance regimes can be costly. Therefore, an organization's cybersecurity program must be well-aligned with its mission and appropriately balance risk with cost and research innovation.

The following sections outline aspects of a suggested framework for the organization's cybersecurity program.

• Mission Alignment

The selected must understand their organization's mission to create an effectively tailored cybersecurity plan which accounts for the impact cybersecurity can have on the organization's mission. For example, investing in preventative cybersecurity can be significantly cheaper than the cost of a cyber incident. However, overinvesting in cybersecurity can have diminishing returns if those funds could have directly advanced the mission.

• Stakeholders and Obligations

Project Teams must identify their cybersecurity stakeholders and account for their cybersecurity obligations. Cybersecurity stakeholders are people or entities with interest in or affected by an organization's cybersecurity program. Internal stakeholders include the cybersecurity operator and IT leadership, application developers, system administrators, and information system users. External stakeholders may include research partners, suppliers, parent organizations, and others.

1. 42 U.S.C. § 18725

- ## Information Asset Inventory

  An organization must identify and locate all their information assets to competently secure them.[2] The inventory should identify the asset, indicate the value or sensitivity of the system, and/or classification of the information. The data management plan submitted with the project proposal is a key source for both asset identification and classification. You can use publicly or commercially available templates or worksheets to build your asset inventory or construct a custom database.

- ## Information Classification

  Information has varying degrees of organizational value, sensitivity, and protection requirements. These are key factors to consider in analyzing the anticipated impact of security incidents. In addition, some information assets may be subject to additional external control (e.g., federal or state privacy laws, international regulations, contractual obligations). In most cases, information can be classified into categories such as public, internal, or controlled.

- ## Roles and Responsibilities

  Successful cybersecurity plans should align with the organization's existing cybersecurity program. The organization's leadership should have an active role in developing cybersecurity policy and implementing the cybersecurity program. Leadership should also be involved in assigning information asset ownership, security roles, and responsibilities.

  An information asset owner is a person, position, or entity given formal responsibility for an information asset (or set of assets) within an organization. This person must ensure adequate controls are in place over the life of the project to protect the asset and its information from threats to confidentiality, integrity, and availability.

  In addition, cybersecurity programs should have an identified senior security role, such as a Chief Information Security Officer or Information Security Officer. This person owns the cybersecurity program and is the lead decisionmaker for its operational aspects. This individual also facilitates the formation of informed cybersecurity policies and risk management decisions by organization's leadership and information asset owners.

- ## Policies

  Every project's cybersecurity program requires the development, approval, and implementation of some information security policies. Examples of common information security policies include an Acceptable Use Policy; Access Control Policy; and Incident Response Policy. These policies are driven by the organizations' information assets and classifications, but also by any applicable regulations.

  Trusted CI, the National Science Foundation's Cybersecurity Center of Excellence, recommends developing a "Master Information Security Policy and Procedures" document as an initial policy-making step and has a set of policy templates available for customization. A master information policy should have an overview of the project's information security program, including a summary of roles and responsibilities, and an organized list of specific information security policy documents. For additional examples of policy templates and forms, see the Higher Education Information Security Council (HEISC) Resources Center, and SANS Institute's Information Security Templates page.

  Using policy templates and examples can streamline your policy creation and drafting, even if substantial customization is required. The policies themselves only reduce risk if attached to other elements of the cybersecurity plan (e.g., roles and responsibilities, controls) and are integrated into overall project governance and management.

- ## Risk Management and Acceptance

  Cybersecurity plans employ a risk-based approach to information security. DOE acknowledges that any valuable activity requires accepting residual risk, the risk that remains in the presence of controls. Due to the rapidly changing technology landscape, a flexible risk assessment process is often more valuable than a formal, detailed risk assessment that can quickly become obsolete.

2. For example, consider Center for Internet Security's Critical Security Controls 1 and 2, https://www.cisecurity.org/controls

In addition to the Trusted CI implementation guide, the Open Science Cyber Risk Working Group has developed and released a best practices document to assist DOE, and other Federally funded projects in assessing cybersecurity risks related to Open Science projects. Finally, the Armed Forces Communications and Electronics Association International Cyber Committee produced a helpful document on the economics of cybersecurity and cybersecurity investment.

- ## Evaluation

  Given the dynamic technology and cybersecurity landscape, selectees should plan for periodic evaluations of their cybersecurity plan, including policies, practices, and controls. DOE oversight involves regular reporting and review of program milestones, outcome metrics, and incidents. The selectee should also consider periodic self-assessments, external or stakeholder reviews, and incident response evaluations. There are tools to aid in assessment, such as HEISC's Information Security Program Assessment Tool and the Idaho National Laboratory's Cybersecurity Evaluation Tool.

- ## Budget

  Overall, worldwide cybersecurity spending is on the rise driven by increased cybercrime and new data protection regulations. There is wide variability in cybersecurity costs depending on the type of institution (*e.g.*, Defense and Aerospace industries have more stringent requirements and proportionally higher costs), the consequences of a cyberattack, and size of the institution (small institutions may not achieve economies of scale).

- ## Personnel

  The key to a successful cybersecurity program is access to skilled cybersecurity professionals. The Chief Information Security Officer may manage a team of dedicated information security professionals or oversee staff/activities in various departments within the organization. There is high demand for experienced cybersecurity professionals, and organizations may need to consider outsourcing security services. Information security resources outside the organization, such as a parent institution, peer organizations, commercial security consultants, intrusion detection and log monitoring services, and incident response services can be an important source of security expertise, training, evaluation, and recommendations.

- ## Controls

  Controls, or mitigations, are the administrative, technical, and physical safeguards and countermeasures implemented by an organization for the protection of their information assets. Controls are tailored to an organization's specific portfolio of information assets, and are aligned to protect confidentiality, integrity, and availability based on the corresponding risk of exploitation. Control selection, implementation and evaluation will be an ongoing process in any information security program.

  For assistance in selecting baseline controls that can be customized, please see the Center for Internet Security's Critical Security Controls, the National Institute of Standards and Technology's Cybersecurity Framework, and the Australian Cyber Security Centre's Essential Eight. Scientific facilities may merit special security considerations (*e.g.*, diverse research data flows; identity management for distributed science communities,[3] non-organization device connectivity to the organization's networks and data; unique Industry Control and/or Supervisory Control and Data Acquisition systems,[4] application[5] software[6] development[7]).

3. *https://refeds.org/sirtfi*
4. *https://www.cisa.gov/uscert/ics/*
5. *https://social.technet.microsoft.com/wiki/contents/articles/7100.the-security-development-lifecycle.aspx*
6. *https://owasp.org/www-project-top-ten/*
7. *https://www.sans.org/cloud-security/#resources/swat*